What is claimed is:

1. A method of detecting intrusions using a host-based intrusion system, comprising:

reading kernel records;

reformatting each of the read kernel records into a different format;

parsing the records and comparing the parsed records against one or more templates.

2. The method of claim 1, wherein the kernel records include kernel audit logs.

3. The method of claim 2, wherein the kernel audit logs includes information about each system call.

4. The method of claim 1, comprising monitoring system log files.

5. The method of claim 1, comprising a system call.

6. The method of claim 1, wherein the system call was initiated by a library call.

7. The method of claim 3, comprising storing each system call in a circular buffer.

8. The method of claim 1, comprising determining that an intrusion has occurred and generating an alert message.

9. The method of claim 1, comprising encrypting information sent between the host-based intrusion system and a network.

10. The method of claim 1, comprising displaying an alert message that an intrusion has occurred.

11. The method of claim 1, wherein the different format is a memory mapped file.

12. The method of claim 4, comprising converting the system log files into an ASCII format for comparison against the one or more templates.

13. The method of claim 2, comprising converting the kernel records into an ASCII format for comparison against the one or more templates.

14. The method of claim 1, wherein the one or more templates is a modification of files/directories template.

15. The method of claim 1, wherein the one or more templates is a change to log files template.

16. The method of claim 1, wherein the one or more templates is a SetUID files template.

17. The method of claim 1, wherein the one or more templates is a creation of world-writables template.

18. The method of claim 1, wherein the one or more templates is a repeated failed logins template.

19. The method of claim 1, wherein the one or more templates is a repeated failed SU commands template.

20. The method of claim 1, wherein the one or more templates is a race conditions attack template.

21. The method of claim 1, wherein the one or more templates is a buffer overflow attacks template.

22. The method of claim 1, wherein the one or more templates is a modification of another user's file template.

23. The method of claim 1, wherein the one or more templates is a monitor for the start of interactive sessions template.

24. The method of claim 1, wherein the one or more templates is a monitor logins/logouts template.

25. The method of claim 1, wherein the one or more templates is chosen from the group including:

a modification of files/directories template;

a change to log files template;

a SetUID files template;

a creation of world-writables template;

a repeated failed logins template;

a repeated failed SU commands template;

a race conditions attack template;

a buffer overflow attacks template;

a modification of another user's file template;

a monitor for the start of interactive sessions template; and

a monitor logins/logouts template.

26. The method of claim 1, wherein the kernel records are read from different computers.

27. The method of claim 1, wherein parsed records are compared against the one or more templates using at least one correlator.

28. The method of claim 1, wherein said parsing step compares the parsed records against the one or more templates simultaneously.

29. A method of detecting changes to critical files/directories, comprising:

monitoring a predetermined set of files for modifications;

monitoring a predetermined set of directories for modifications;

generating an alert for each occurrence of a modification of a monitored file; and

generating an alert for each occurrence of a modification of a monitored directory.

30. The method of claim 29, comprising:

determining which files to monitor of all files on a computer to form the predetermined set of files;

determining which directories to monitor of all directories on a computer to form the predetermined set of directories.

31. The method of claim 29, comprising, for each said determining step, specifically including a file or directory, specifically excluding a file or director, or not specifically including or excluding a file or directory.

32. The method of claim 29, wherein a file or directory which is not specifically included or excluded is monitored.

33. The method of claim 29, wherein if a directory is specifically excluded and a file in the specifically excluded file is specifically included then the file is monitored.

34. The method of claim 29, wherein the predetermined set of files includes a system kernel file and system kernel configuration files.

35. The method of claim 29, wherein the predetermined set of files includes /stand/vmunix, /stand/kernel and /stand/bootconf.

36. The method of claim 29, wherein the predetermined set of files includes files defining the users on a system and files used to create accounts.

37. The method of claim 29, wherein the predetermined set of files includes /etc/passwd and /etc/group.

38. The method of claim 29, wherein the predetermined set of files includes files which control what network services are running and which controls programs used to fulfill service requests.

39. The method of claim 29, wherein the predetermined set of files includes /etc/inetd.conf.

40. The method of claim 29, wherein the predetermined set of files includes files which are used to control the remote access of the user root without requiring a password.

41. The method of claim 29, wherein the predetermined set of files includes/.rhosts and /.shosts.

42. The method of claim 29, wherein the set of files specifically excluded includes temporary files created by a program view.

43. The method of claim 29, wherein the predetermined set of directories includes /bin, /sbin and /usr/bin.

44. A method of detecting changes to log files, comprising:

monitoring a user defined list of files for attempts to modify any of the files in any way other than appending.

45. The method of claim 44, wherein the user defined list includes:

/var/adm/utmp

/var/adm/btmp

var/adm/wtmp

/etc/utmp

/etc/btmp

/etc/wtmp

46. A method of detecting intrusions, comprising:

monitoring repeated failed login attempts; and

generating an alert if a predetermined threshold is exceeded.

47. A method of detecting a race condition attack, comprising:

monitoring file accesses that a privileged program performs; and

generating an alert if an inode for a file reference appears to have unexpectedly changed.

48. The method of claim 47, wherein a list of users being monitored includes root, daemon, bin, sys, adm, uucp, lp, nuucp.